SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- international: G06F13/00; G06F15/00; H04L9/00; H04L9/00; H04L9/10; H04L9/12

- european: G06F1/00N7R2; G06F9/445; G06F9/445N; G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

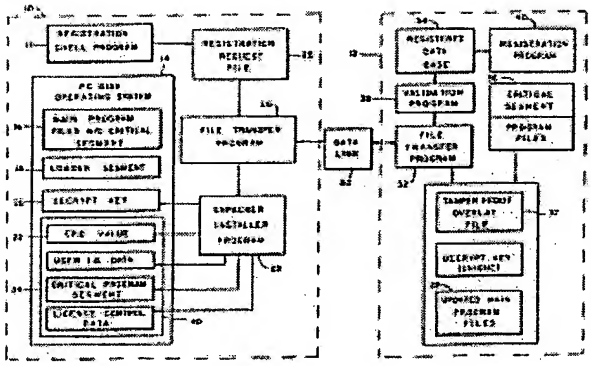
WO9209160 (A1)
EP0556305 (A1)
US5222134 (A1)
EP0556305 (A4)
EP0556305 (B1)

more >>

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平6－501120

第６部門第３区分　(43)公表日　平成６年(1994)２月３日

(51)Int.Cl.'		識別記号	庁内整理番号	Ｆ Ｉ
Ｇ０６Ｆ	13/00	３５１	Ｈ 7368－5Ｂ	
	15/00	３３０	Ａ 7459－5Ｌ	
Ｈ０４Ｌ	9/00			
	9/10			
			7117－5Ｋ	Ｈ０４Ｌ 9/00 Ｚ

審査請求　有　予備審査請求　有　（全８頁）　最終頁に続く

(21)出願番号　特願平4－501845
(86)(22)出願日　平成３年(1991)11月６日
(85)翻訳文提出日　平成５年(1993)５月７日
(86)国際出願番号　ＰＣＴ／ＵＳ９１／０８０６９
(87)国際公開番号　ＷＯ９２／０９１６０
(87)国際公開日　平成４年(1992)５月29日
(31)優先権主張番号　６１０，０３７
(32)優先日　1990年11月７日
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６８２，４５６
(32)優先日　1991年４月９日
(33)優先権主張国　米国（ＵＳ）

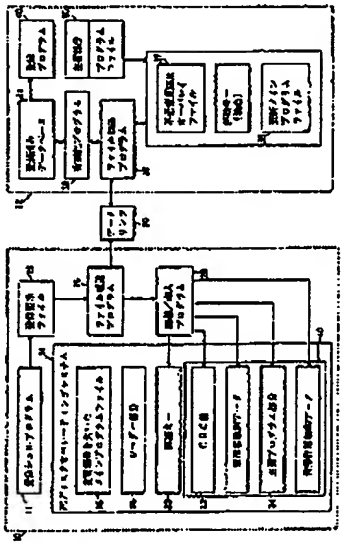
(71)出願人　タウ　システム　コーポレイション
アメリカ合衆国　バージニア州　フォルス　チャーチ，リースバーグ　パイク，7115，スーツ327
(72)発明者　ワイト，デービット，ビー
アメリカ合衆国　バージニア州　22032，フェアファックス　ギルバートソン　ロード，4220
(72)発明者　リッデル，ホレイス，ジー
アメリカ合衆国　バージニア州　22021，チャンチリイ，バレイ　カウントリ　ドライブ，13811
(74)代理人　弁理士　倉持　悟　（外１名）

最終頁に続く

(54)【発明の名称】　パーソナルコンピュータのソフトウエアを遠隔位置で起動するための安全システム

(57)【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルプログラム(11)が当初備わっている。データリンク(30)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾識別データと使用許諾制御データも含まれている。



【請求の範囲】

1．プログラムファイルを制御する方法であって、

書換装置を有する遠隔コンピュータに対して、ローダーセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは主要部分を欠いていて、上記プログラムファイルを正しく実行することを防止する工程、

使用者識別情報を上記登録シェル部分に入力する工程、

上記使用者識別情報を、上記登録シェルから登録用コンピュータ内にある独立した登録プログラムに伝送し、上記登録プログラムは使用者識別データと上記主要部分とを結合して独自のオーバーレイファイルを作成する工程、

上記の独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝送する工程、上記オーバーレイファイルには上記プログラムファイルには当初欠けている主要部分が含まれ、そして

上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用者識別が導入されたときだけ上記プログラムファイルの動作を可能とすることを特徴とする前記のプログラムファイル起動方法。

2．上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝送する前に、上記使用者識別情報を利用可能にする工程を有する請求の範囲第1項に記載の方法。

3．不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。

4．上記不正変更防止オーバーレイファイルが上記オーバレイファイルを暗号化することにより作成され、巡回冗長検査値が上記暗号化オーバーレイファイル内にあるとともに、解読キーを上記オーバーレイファイルに供する請求の範囲第3項に記載の方法。

5．上記オーバーレイが実行のためにロードされるたびに巡回冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以後変更されているかどうかを判断することを特徴とする請求の範囲第4項に記載の方法。

6．上記使用者識別情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シェルと上記登録プログラムとの間を伝送されることを特徴とする請求の範囲第1項に記載の方法。

7．上記登録シェルプログラムが、上記の独立した登録用コンピュータを備えた第二の遠隔コンピュータから離れた、第一のコンピュータ内に設けられていることを特徴とする請求の範囲第1項に記載の方法。

8．上記利用可能工程によって上記使用者識別情報が正式の登録シェルを保証することを特徴とする請求の範囲第2項に記載の方法。

9．上記使用者識別と上記オーバーレイファイルが、一台のコンピュータに入力され備えられることを特徴とする請求の範囲第1項に記載の方法。

10．プログラムファイルを制御されたもしくは制限されない利用可能するためのシステムにおいて、

オーバーレイローダー部分が含まれているが少なくとも一つの主要プログラム部分が欠けているプログラムファイルが当初備わっていて、このプログラムファイルが動作することを防止し、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が様々な使用者識別情報を入力することを可能にするような少なくとも一台の遠隔コンピュータと、

登録プログラムと、上記使用者識別情報を受信し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用者識別情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用者識別が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

11．上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル転送処理とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

12．上記登録用コンピュータが、すべての登録済み使用者が含まれている中央データベースと上記使用者識別情報を有効化するための手段とを備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

13．オーバーレイファイルを作成するための上記手段が、巡回冗長検査値を備える不正変更防止オーバーレイファイルを作成するための暗号化装置と解読キーを備えており、上記解読キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14．上記遠隔コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第13項に記載のプログラムファイル起動システム。

15．上記主要部分がエグゼクティブ制御部分であり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16．上記主要プログラム部分がエグゼクティブ制御プログラムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル制御システム。

17．上記主要エグゼクティブ制御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル制御システム。

18．　プログラムファイルの使用を制御する方法において、

書換装置を有するコンピュータに対してローダー部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

ファイルは第一レベルの制御機能を有するエグゼクティブ制御プログラムを有しており、

情報を上記登録シェル部分に入力し、

上記使用許諾契約情報を上記登録シェルから独立登録プログラムに伝送し、上記登録プログラムに使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに併合して独自のオーバーレイファイルを発生し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自オーバーレイファイルを上記主要プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が現在導入されているときだけ可能になること特徴とする上記のプログラムファイル使用の制御方法。

19. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

20. 不正変更防止になっているオーバーレイファイルを作成する工程を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査値を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに解読キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化および解読キーは上記オーバーレイファイルの独自の内容によって独自に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録シェルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするような少なくとも一台の遠隔コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全部あるいは一部を含む独自のオーバーレイファイルを形成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在備わっているときだけ、上記プログラムファイルの第二レベルの機能動作が可能なることを特徴とする上記システム。

28. 上記遠隔コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送過程が上記登録用コンピュータと上記遠隔コンピュータの両方に備えられていることを特徴とする請求の範囲第27項に記載のシステム。

29. 上記登録用コンピュータが、すべての登録済み使用者が含まれる中央データベースと上記使用許諾契約情報をお処化する手段とを備えていることを特徴とする請求の範囲第27項に記載のシステム。

30. オーバーレイファイルを形成するための上記手段が、巡回冗長検査値が記憶されている不正変更防止オーバーレイファイル作成するための暗号化キーと解読キーとを備えており、上記解読キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送され、上記暗号化および解読キーはファイルの内容によって独自に決定されることを特徴とする請求の範囲第27項に記載のシステム。

32. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に供給された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第31項に記載の方法。

33. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録シェルと上記登録プログラムとの間を電子データリンクを介して伝送されることを特徴とした請求の範囲第18項に記載の方法。

34. 上記登録シェルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに備えられていることを特徴とする請求の範囲第18項に記載の方法。

35. 上記有効化により上記使用許諾契約情報が正式の登録シェルを介して保存することを特徴とする請求の範囲第19項に記載の方法。

36. 上記使用許諾契約情報と上記オーバーレイファイルが一台のコンピュータに入力され、備えられることを特徴とする請求の範囲第18項に記載の方法。

37. 制限されたあるいは制限されない初回、プログラムファイルをアップグレイドするシステムにおいて、

第一レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが含まれており、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、

システム。

31. 上記遠隔コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに新しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第30項に記載のシステム。

【明細書】

パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

発明の背景

一般的に、パーソナルコンピュータあるいはそれに類似した装置の使用者の大部分は、それら装置で実行するソフトウェアを様々な小売店からあるいは通信販売を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「収縮包装」材で包装されており、その収縮包装材を破った時点でそのソフトウェア製品に対する使用許可契約が成立して、その製品の使用許諾者を被使用許諾者／購入者による無許可複製あるいは使用から保護するようになっている。この方法による商行為は、許諾者と被許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、被許諾者にとっては、ソフトウェアプログラムを動作させてみてからそれが被許諾者が必要としているものかどうかを判断する機会が与えられない。さらに、許諾者の側からみると、この方法では被許諾者の識別ができないうえ、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアプログラム保護方式は、Thomasの米国特許第4,446,519号に複数開示されており、プログラミングされた「はい／いいえ」で答える設問がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに設置されているハードウェアあるいはファームウェア保護装置の存在を確認するようになっている。この技法の意図は、プログラムが物理的な保護装置なしでは使用できないようにすることであり、これはソフトウェアよりも複製することがはるかに困難である。しかし、このような技法は、正しい符号化応答が見破られ、そしてそれをわずかに変更してプログラムに書き込まれてしまえば、簡単に打ち破られてしまう。ひとたび打ち破られると、無制限の違法コピーが作成され配布される可能性がある。

Williamsの米国特許第4,740,890号は、中央（遠隔）コンピュータを使用して、正しい符号の入力を試みる悪意のプログラマがアクセスできないマスターリストあるいはアルゴリズムから得られたコンプ保険コードあるいは有効化コードを提供することを開示している。しかし、この方法は、仮想字のコードを傍受することにより、あるいは保護の問題をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つけ出すことにより、簡単に突破られてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの無制限のコピーが作成され配布される可能性がある。

さらに、Schoidtの米国特許第4,649,510号に開示されている方法では、最も価値のあるアルゴリズムを無効化し、無効化されたプログラムを処理装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離し保護された処理装置で実行することにより回復し、有効結果を2つの処理間の相互通信によって獲得するようになっている。このような技法は、回復アルゴリズムの物理的保護に依存しており、この物理的保護が侵害された場合、悪意のプログラマによって簡単に打ち破られる可能性がある。したがって、そのような方式は、回復記憶装置の物理的保護が維持できない大量市場においては、実用的ではない。

そのため、ソフトウェアを無許可使用から保護しつつソフトウェアを大量市場に配布するための経済的な方法が求められる。さらに、見込み購入者／被許諾者がソフトウェア製品を購入前に試してみることができような方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分を登録使用者に配布するための方法も必要である。

発明の簡単な説明

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理した方法で配布する方法とシステムに関する。動作可能プログラムは、購入者／被許諾者と販売者／許諾者との間の特定の契約において入手可能になる。販売者と購入者との関係は、本発明の目的に関しては、許諾者／被許諾者契約の関係である必要はないが、以下では販売者を許諾者、購入者を被許諾者もしくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に合意すると、被許諾者識別データが登録用コンピュータに与えられる。登録用コンピュータはその契約を記録し、使用許可されたプログラムの可動部分を提供する。これらの部分は不正変更防止が施されていると同時に、識別された被許諾者にとって独自のものとなっている。この情報の交換に基づき、可動コンピュータプログラムが登録済み被許諾者のコンピュータに不正変更防止ファイルに収納されて配布される。同時に、このファイルには被許諾者独自の情報が含まれている。本発明の実施例としては様々なものが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する指示とが含まれている暗号化パッケージの構成を持っている。したがって、被許諾者は顧客ではなく、そして保護されたソフトウェアは使用許可契約に追及できる情報で符号化される。さらに、使用許可制御データを暗号化パッケージに含めることにより、様々な制限を課して使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシェルプログラムの最初の起動が伴う。このシェルプログラムは、見本説明と宣伝記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローダーセグメントと呼ばれる特別のプログラムモジュールを含むような構成になっている。

マーケティングシェルは適切な方法で自由に配布されるであろう。マーケティングシェルがプログラムのデモンストレーション版を有している場合、エグゼクティブ制御ループが保護されたプログラムの限定版になる。マーケティングシェルは見込み使用者に登録を促す。マーケティングシェル内の登録プログラムは、登録データを登録データベースコンピュータに中継する。暗号化ファイル内で結合された被許諾使用者独自のデータと動作可能版のプログラムとを有する独自の暗号化パッケージが組み立てられる。独自の暗号解読キーが、暗号化ファイルおよび保護されていないプログラムファイルと共に使用者のコンピュータに伝送されるが、これらはマーケットシェルを増大させる。解読キー、暗号化ファイル、そして保護されていないファイルの到着と同時に、マーケットシェルはこれらの各々を使用者のコンピュータに導入する。

したがって、使用者がプログラムを実行する毎に、ローダセグメントが供給された解読キーを使用して、暗号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解読する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているプログラムはその暗号化形態に留まって、保護されていないプログラムファイルと共にコンピュータの大容量記憶装置に格納されている。保護されているプログラムは実行のためにロードされたときだけ解読され、正しい暗号化キーにアクセスしなければ変更され得ない。

図面の簡単な説明

図1は本発明による登録過程を示す流れ図である。

図2は本発明によるプログラム実行過程を示す流れ図である。

図3は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータの概略図である。

図4は、本発明の知見による代表的なパーソナルコンピュータと登録用コンピュータに代る実施例を示す概略図である。

発明の詳細な説明

本発明の目的は、許諾者がそのプログラムの費用対効果に関する費用を従来使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る際に試用することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾保証されたアップグレイド版を登録被許諾者に配布する手段を提供することである。したがって、本発明の知見は包括的なものと考えられ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと意図されている。

一実施例において、動作可能なエグゼクティブ制御ループを除いて完全な特定プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、ファームウェア、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定プログラムには登録シェルプログラムも含まれる。ただし、小さいプログラムもしくは著しく低価のあるプログラムの場合、プログラム自体は存在せず、シェルだけが提供される。エグゼクティブ制御ループが除外されているため、このプログラムは正しい登録過程を実現しなければ動作しない。図1および図3に示されているように、この登録過程は、パーソナルコンピュータ(PC)10内部の登録シェルプログラム12と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ18内に提供され、電子データリンク30を介して登録シェルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる種類であってもよい。ただし、第二の実施例においては、登録シェルおよび登録システムプログラムは同一の媒体上に存在してもよいが、その媒体は製品応用プログラムとは別でなければならない。この場合、登録シェルおよび登録システムプログラムが入っている再使用可能な媒体は、許諾された購入プログラムによって使用者パーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シェルプログラムは、使用者がPCオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行を最初に試行すると実行される。登録シェルは、製品応用プログラムに関する認証情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促して価格者として登録する。使用許諾は、特定の使用場所における特定の被許諾者に対して確認され、その期間は恒久的なものもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シェルは、不正変更防止オーバーレイファイルが存在しないかぎり、メインプログラムを実行しない。登録シェルプログラム11は、被許諾者のPCに表示されるデータ入力形式を提供し、被許諾者に対して、顧客番号特定、口座番号、使用許諾条件などの識別情報の提供を要求する。この情報は、被許諾者が再確認する登録要求ファイル35に入力される。そして、登録シェルプログラムに、被許諾者が指定キーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが開き、そして登録シェルファイル転送プログラム26が登録システムファイル転送プログラムとのデータリンクを確立する。登録用コンピュータ内の登録プログラム40は、データリンクが正当な登録シェルで確立されていることを確認する検密保護チェックを実行する有効化手段42によって保護される。つぎに、登録シェルは登録要求ファイル35を、そのファイルを受信する登録システムに転送し、必要なエラーチェックと、結合されたファイル転送プログラム26および32間のハンドシェーク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録済み使用者94のデータベースに対して照合される。照合には、その要求に答えるべきかどうかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのエグゼクティブ制御ループは送信されない。そのような状態が発生した場合、適切なメッセージが登録シェルに転送され、見込み被許諾者に対して表示される。しかし、要求が確認されると、登録済み使用者データベースへの記録が作成されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ32の内部では、つぎに使用者識別データが使用されて、使用者識別データとエグゼクティブ制御ループプログラム命令36とを併合することにより作成された独自の不正変更防止オーバーレイファイルが作成される。併合されたデータとプログラムファイルに独自で、不正変更防止オーバーレイファイル37内に含まれる巡回冗長検査(CRC)値が計算される。一式の独自の暗号化キーと解読キーが作成され、不正変更防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正変更防止オーバーレイファイルと共に保護される解読キーが提供される。暗号化アルゴリズムは、公開鍵暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する仕様であればなんでもよい。登録システムが、不正変更防止オーバーレイファイルと解読キーを、パーソナルコンピュータ登録シェルに伝送される1個の出荷ファイル38に組み込む。また、更新されたメインプログラムファイルもこの出荷ファイルに組み込まれ、ファイル転送プログラムとすでに確立されているデータリンクとを通じてPCの登録システムに伝送される。

出荷ファイル一式の受信と同時に、登録シェルプログラム内の開梱ー導入プログラム44が出荷ファイルを開き、エグゼクティブ制御ループセグメント34、CRC値22ならびに解読キー20および、含まれている場合は、更新メインプログラムファイルを含む不正変更防止オーバーレイファイル40を導入する。これで登録過程が完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する解決が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された記憶済み製品応用プログラムを起動して、不正変更防止オーバーレイファイルと解読キーを使用して製品応用プログラムを実行するたびに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図3に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つぎに、ローダーセグメントは製品応用プログラムの起動を実行し、不正変更防止オーバーレイの存在をチェックする。不正変更防止オーバーレイが導入されていなければ、ローダーセグメントは終了してオペレーティングシステムに戻るので、メインプログラムファイルの実行が事前に防止される。不正変更防止オーバーレイが導入されていれば、ローダーセグメントは解読キーを見つけて不正変更防止オーバーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティブ制御ループプログラム命令ならびに独自の識別および使用許諾制御データを重ね合せる。解読およびロード過程において巡回冗長検査が実行され、それが完了すると、不正変更防止オーバーレイが登録用コンピュータからパーソナルコンピュータに伝送されたときに作成された不正変更防止オーバーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査が失敗に終わると、そのオーバーレイは何らかの方法によって変更が加えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグメ

ントはそのオーバレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバレイのどの部分が変更されていても、事前に防止される。巡回冗長検査の結果、オーバーレイが変更されていないことが確認されると、ローダーセグメントはオーバレイを含めたメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能形態の製品応用プログラムに含めることを要求することにより、被許諾者識別と使用許諾制御データはそれ以降動作可能プログラムに常に含められることになる。このようにして、許諾者は不正使用を防止するとともに実施することができる。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのエグゼクティブ制御ループセグメントと使用許諾制御データとを含む不正変更防止オーバーレイファイルが作成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動後に不正使用を防止するキー装置である。なぜなら、エグゼクティブ制御ループプログラム命令は、分岐なしには独自の使用許諾識別データと使用許諾制御データから分離することもできなければ、被許諾者識別と使用許諾制御データも発覚なしには変更できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが使用されるときに最初に巡回冗長検査値をオーバーレイファイルに記憶させることで不正変更防止になるとみなされる。巡回冗長検査値は、プログラム命令と使用許諾データを含むオーバーレイファイルの内容全体に対して計算される。被許諾者データは独自であるので、各々のCRCは独自なものになる。記憶されているCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された巡回冗長検査値と比較される。これらの巡回冗長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容になんらかの変更が加えられていれば、記憶されている巡回冗長検査値に対応する変更が行われないかぎり、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、巡回冗長検査値の位置が不明になるような方法で暗号化されるので、この値の所在をつきとめてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令ならびに独自の使用許諾識別および使用許諾制御データがはっきりしなくなる。暗号化は、公開鍵暗号化システムのように暗号化と解読に別々のキーを使用する技法によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発生のためのアルゴリズムは登録システム内に常駐し、したがって被許諾者にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルを通じて被許諾者のコンピュータに転送される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、困難ではあるが可能である。しかし、内容を変更して、新しい変更された不正変更防止オーバーレイファイルを暗号化する技法は、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけしか公共相補解読キーで解読できず、私的キーは公共キーから容易には得られないというのが、公共鍵暗号システムの一特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ループセグメントと、使用許諾の方法と制御に適切な個々の使用者識別データとを有している。このデータには、使用許諾の期間、コンピュータの製造番号、コンピュータのモデムの電話番号、そしてその他の情報が含まれる。

ローダーセグメント18は特殊目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり迂回された場合、メインプログラムファイルを動作不能にする技法によって製品応用プログラムのメインプログラムファイルに結合される。この結合技術は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、使用者にとっては既知の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の機能の他にこの動作を実行する。したがって、ローダーセグメントを取り外したり迂回したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

別の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許諾データは含まれないが、登録版の製品の機能と同様のデモンストレーションだけを行なうメインプログラムエグゼクティブ制御ループが含まれるであろう。デモンストレーション版のエグゼクティブ制御ループは、エグゼクティブ制御ループの設計段階によって組み込まれたプログラムの様々な機能を有している。たとえば、選択肢を提供するデモンストレーションメニューをプログラミングして選択肢を表示することができるが、デモンストレーション版のエグゼクティブ制御ループをプログラミングして選択項目を製品登録依頼として解釈して、製品を動作させる前に登録することを要求できる。

登録を開始する前に、見込み被許諾者はプログラムを実行し、デモンストレーション版が実行されるであろう。指定しそして図3に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ループがロード、解読、そして実行される。デモンストレーションが終了すると、見込み使用者は、使用者として登録し登録版のプログラムを実行するための一時的使用許諾を得るように促される。そして、使用者は前述のようにして登録を行い、図4に示されているプロセスを開始することができる。登録要求に応答して、新しいオーバーレイファイル40'と独自の解読キー20'が含まれている応答ファイルが登録用コンピュータから送られる。追加プログラムファイルと更新版のプログラムファイルも、応答ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20をそれぞれの登録値40'と20'で置き換えをする。

登録に続き、使用者がプログラムを実行すると、プログラム実行過程で登録済み版の不正変更防止オーバーレイ40'が検出されてロードされ、独自の解読キー20'を使用することにより、登録済み版のエグゼクティブ制御ループが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に変換される。

プログラムの機能向上版が利用できる場合、使用者は同一のプロセスを起動してさらに別の解読キーと、より強化されたエグゼクティブ制御ループと追加プログラムファイルを有する別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することができる。

様々な実施例が、今や様な不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための適切で独創的な技法を供

用することができる。このような技法は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用許諾契約と結合する形式で配布するための、ここに開示されている方法がもたらす両面防御法の可能性の単なる例である。

上記の知見に照らし合わせ、本発明に様々な変形例が可能なことは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、さらにその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように階層構造内に実現することも可能である。その地域の登録用コンピュータの登録機関は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの契約に含まれる使用許諾制御データによって制御できるであろう。したがって、下記の特許請求の範囲内であれば、本発明を上記明細書に説明されている以外の方法で実施することができる。

図 1

登録過程

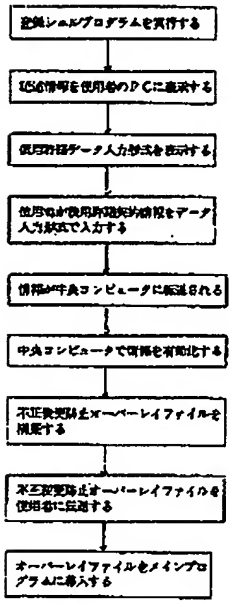
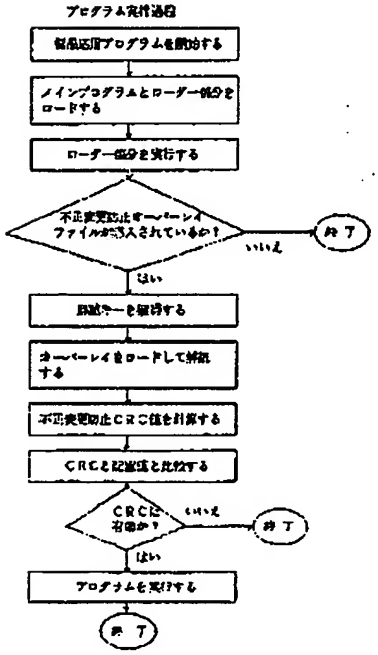
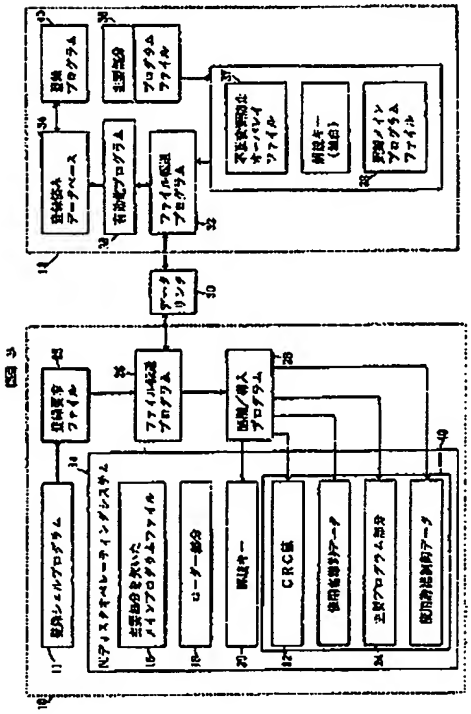
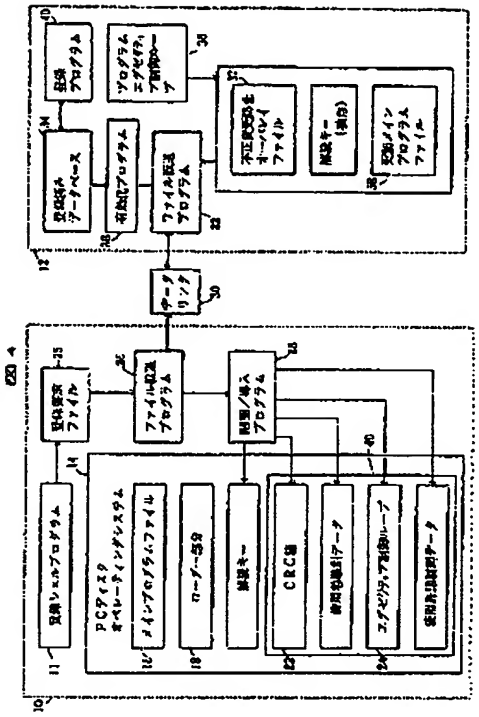


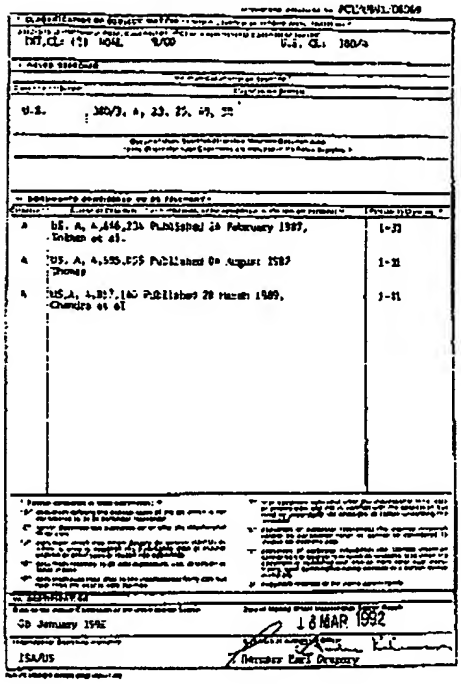
図 2

プログラム実行過程









フロントページの続き

(51)Int.Cl.[5] 識別記号 庁内整理番号 FI
H04L 9/12

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, SE), CA, JP